



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,624	05/14/2001	Daryl Carvis Cromer	RPS919980030US2	9643

25299 7590 10/18/2005

IBM CORPORATION
PO BOX 12195
DEPT YXSA, BLDG 002
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER

REFAI, RAMSEY

ART UNIT PAPER NUMBER

2152

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

OCT 18 2005

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/855,624
Filing Date: May 14, 2001
Appellant(s): CROMER ET AL.

John L. Rogitz
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed July 17, 2005 appealing from the Office action mailed June 23, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,119,234	Aziz et al	9-2000
5,857,072	Crowle	1-1999

- *Microsoft Computer Dictionary*, 5th Edition, Redmond, Washington, Microsoft Press, 2002, pp. 513
- Feit Sidnie, *TCP/IP*, McGraw Hill, 1997, Chapter 12

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

- 1. Claims 10-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Aziz et al (U.S. Patent No. 6,119,234). This rejection was set forth in the previous office action mailed June 23, 2005.**

As per claim 10, Aziz et al teach a method for providing update configuration data for a client personal computer system in a data network including a server, having configuration data including an internet protocol destination address, and at least one client personal computer system having a storage device for storing configuration data and a micro controller for receiving network signal packets from the server and for configuring the client personal computer system with updated configuration data, including the internet protocol destination address of the server, comprising the steps of: receiving a network signal packet sent from the server in the micro controller in the at least one client personal computer system (**column 2, lines 52-58**); determining that the network signal packet includes the server's Internet protocol destination address (**column 3, lines 38-50**); determining that the network signal packet is a match for the any one of the at least one client personal computer system (**column 3, lines 14-29, 52-58 and column 9, lines 12-25; authentication**); and responding to the receiving, determining inclusion of the server's address (**column 2, lines 52-58, column 3, lines 38-50**) and determining that the packet is a match by updating the storage device of the any one of the at least one client personal computer system with the Internet protocol destination address of the server included in the

packet (column 3, lines 14-29, 52-58 and column 9, lines 12-25; authentication column 2, lines 52-60).

As per claim 11, Aziz et al teach after the step of receiving the network signal packet, there is a step of authenticating the encryption of the network signal packet to authenticate the presence of encrypted data in the network signal packet (column 3, lines 14-29, 52-58 and column 9, lines 12-25).

As per claim 12, Aziz et al teach after the step of authenticating the encryption of the network packet, there is a step of validation of the data authenticated in the step of authenticating the encryption of the network packet (column 3, lines 14-58 and column 9, lines 12-25).

As per claim 13, Aziz et al teach determining that the network signal packet includes the servers internet protocol destination address, the presence in the network signal packet of configuration identification and configuration data is determined (column 3, lines 14-58 and column 4, lines 3-6).

2. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz et al (U.S. Patent No. 6,119,234) in view of Crowle (U.S. Patent No. 5,857,072). This rejection was set forth in the previous office action mailed June 23, 2005.

As per claim 14, Aziz et al fail to teach the step of determining whether the network signal packet is a match for any one of the at least one client personal computer system, there is a first determination as to whether the network signal packet is identified to any one of the least

one client personal computer systems and a second determination as to whether the network signal packet is identified to a plurality of client personal computer systems. However, Crowle teaches determining which of the multiple locations is to receive a data distribution. The multiple network computer locations then determine whether it is an intended location for receiving the data distribution (**column 3, lines 10-39**). It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to combine the teachings of Aziz et al and Crowle because Crowle's use of determining whether a computer system is an intended receiver of a data distribution would enhance Aziz et al's method by allow for client computer's to determine if an update of configuration data is intended for that client computer in order to avoid unwanted updates that can lead to loss of accurate configuration data.

As per claim 15, Aziz et al teach a method for providing update configuration data for a client personal computer system in a data network including a server, having configuration data including an internet protocol destination address, and at least one client personal computer system having a storage device for storing configuration data and a micro controller for receiving network signal packets from the server and for configuring the client personal computer system with updated configuration data, including the internet protocol destination address of the server, comprising the steps of: receiving a network signal packet sent from the server in the micro controller in the at least one client personal computer system (**column 2, lines 52-58**);

authenticating encryption of the network signal packet to authenticate the presence of encrypted data in the network signal packet; determining that the network signal packet includes the server's Internet protocol destination address (**column 3, lines 38-50**); and responding to the receiving, determining inclusion of the server's address (**column 2, lines 52-58, column 3, lines**

38-50) and determining that the packet is a match by updating the storage device of the any one of the at least one client personal computer system with the Internet protocol destination address of the server included in the packet (**column 3, lines 14-29, 52-58 and column 9, lines 12-25; authentication column 2, lines 52-60**).

Aziz et al fail to teach the step of determining whether the network signal packet is a match for any one of the at least one client personal computer system, there is a first determination as to whether the network signal packet is identified to any one of the least one client personal computer systems and a second determination as to whether the network signal packet is identified to a plurality of client personal computer systems. However, Crowle teaches determining which of the multiple locations is to receive a data distribution. The multiple network computer locations then determine whether it is an intended location for receiving the data distribution (**column 3, lines 10-39**). It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to combine the teachings of Aziz et al and Crowle because Crowle's use of determining whether a computer system is an intended receiver of a data distribution would enhance Aziz et al's method by allow for client computer's to determine if an update of configuration data is intended for that client computer in order to avoid unwanted updates that can lead to loss of accurate configuration data.

(10) Response to Argument

The Examiner has noticed that in Appellant's response, there are instances of improper decorum and courtesy to the examiner and their supervisor. Such instances are: "the examiner refuses to recognize right answer when told", "the SPE who signed out the Office

Action stubbornly insists”, “the SPE has vetted the last response, it would be highly inappropriate for him to authorize reopening prosecution and thus short-circuiting the appellate process”, and “the SPE studiously ignores” are all found on page 5 of the Appellant’s response. Also on page 6, more instances are found, such as: “Perhaps most damning of the SPE’s case” and “Nothing is more unhinged from reality”. These types of statements are inappropriate and not appreciated. Appellant is reminded of patent rule 37 C.F.R. 1.1, which states:

“Applicants and their attorneys or agents are required to conduct their business with the United States Patent and Trademark Office with decorum and courtesy. Papers presented in violation of this requirement will be submitted to the Director and will not be entered. A notice of the non-entry of the paper will be provided. Complaints against examiners and other employees must be made in correspondence separate from other papers.”

- 1. Appellant argues in substance that Aziz et al mentions nothing about packets and that packets are not inherent because communication can occur without packets.**

In response, Examiner respectfully disagrees. The Appellant is referencing an Ethernet/LAN network using TCP/IP Internet Protocol (see Appellant’s specification pages 3 and 9). Although Aziz et al does not explicitly use the word “packet”, Aziz et al does teach that an address of a domain name server is sent to a client and stored on the client device as a configuration file (see Figure 2A, column 1, line 50 - column 2, line 67, column 5, lines 23-28, column 8, lines 15-25). One skilled in the art would recognize that in order to send any information over a LAN network or any other Internet Network using TCP/IP, which uses

packet-switching technology, the information is always broken into packets and reassembled at the receiving end.

Webopedia states that packet switching *“Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.”* Microsoft Computer Dictionary 5th Edition states that TCP is *“the protocol within TCP/IP that governs the breakup of data messages into packets to be sent via IP (Internet Protocol), and then reassembly and verification of the complete message from packets received by IP.”*

Aziz et al teaches the use of the Internet, LAN/WAN networks and also incorporates by reference Sidnie Feit author of *TCP/IP*, McGraw Hill (1997), Chapter 12, which discusses TCP/IP technology. (see column 2, lines 40-44, column 4, lines 50-55). Therefore Aziz et al meets the claimed scope of the claimed limitation by inherently teaching a packet.

2. Appellant argues in substance that Aziz et al fails to teach storing a server packet at a client.

In response, the Examiner respectfully disagrees because Aziz et al teach that a name server's address is stored in a configuration file on the client. Organizations must designate name servers for each client within an organization. These organizations send the address of the designated name server to the client device. The address is then stored in a configuration file on the client. When a client needs to contact a host at another location, the client would need the host's address. If the host's address is not stored on the client, a resolver program running on the

client, can contact the name server to obtain the host's address by obtaining the name server's address from the configuration file and forwarding the query to the name server. Once the name server obtains the requested host address, a message responding to the query, is sent from the name server to client device. The client device then stores the message. The message contains header information, in which one skilled in the art would know, contains destination address and source address. The message also contains the requested host address. Although Aziz et al does not explicitly use the word "packet", one skilled in the art would recognize that in order to send any information over a LAN network or any other Internet Network using TCP/IP, which uses packet-switching technology, the information is always broken into packets and reassembled at the receiving end. (See Figure 2A, column 1, line 50 - column 2, line 67, column 5, lines 23-60, column 8, lines 15-25).

3. Appellant argues in substance that Aziz et al fails to teach determining that the packet contains the server's IP address.

In response, the Examiner respectfully disagrees because Aziz et al teach a client, requesting the address of a host at another location, can obtain the host address by sending the query to a name server. This is done using a resolver program on the client that determines the name server's address by checking a configuration file located on the client. The resolver program then forwards the query to the name server. Once the name server obtains the requested host address, a message responding to the query, is sent from the name server to client device. The message contains header information, in which one skilled in the art would know, contains destination address and source address. The message also contains the requested host address, the authority,

and additional information. The client device determines that the message is from the authoritative name server and also uses other secure methods to ensure that the message is secure. The client device then stores the message and can then determine the address of the host. (See **Figure 2A, column 1, lines 50-67, column 2, line 45-67, column 5, lines 23-60, column 8, lines 15-25**).

4. Appellant argues in substance that Aziz et al fails to teach updating a configuration file using a packet.

In response to Appellant's arguments, the recitation *updating a configuration file using a packet* has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). Although no patentable weight is given to this recitation, Aziz et al does teach that a configuration file that contains the address of the protected host stored on authorized clients is updated every time the address of the protected host is changed via the LAN/Internet (i.e. packet). (see **column 2, lines 50-67**)

5. Appellant argues in substance that Examiner contradicts himself by admitting that Aziz et al fails to perform the claimed match despite alleging the opposite in the anticipation rejection.

In response, the Examiner respectfully disagrees that the examiner is contradicting

himself. Appealant is not reading points 10 and 13 of the Final Rejection Office Action in its entirety. Examiner has not used the Crowle reference due to the failure of the Aziz et al reference to teach the claimed match but rather due to Aziz et al's failure to teach *a first determination* as to whether the network signal packet is identified to any one of the least one client personal computer systems and *a second determination* as to whether the network signal packet is identified to a plurality of client personal computer systems.

Point 10 in the Final Rejection Office Action recites:

“ 10. As per claim 14, Aziz et al fail to teach the step of *determining whether the network signal packet is a match for any one of the at least one client personal computer system, there is a first determination as to whether the network signal packet is identified to any one of the least one client personal computer systems and a second determination as to whether the network signal packet is identified to a plurality of client personal computer systems.* ”

Point 13 in the Final Rejection Office Action recites:

“13. Aziz et al fail to teach the step of *determining whether the network signal packet is a match for any one of the at least one client personal computer system, there is a first determination as to whether the network signal packet is identified to any one of the least one client personal computer systems and a second determination as to whether the network signal packet is identified to a plurality of client personal computer systems.* ”

Examiner has stated that Aziz et al does teach matching by the use of privacy, integrity and authenticating techniques in order to provide secure communications between a host and a client. To do so, packets that identify a host/client would need to be matched/validated in order

Art Unit: 2152

to verify that the client/host and the communications between them are secure. (see column 3, lines 14-50).

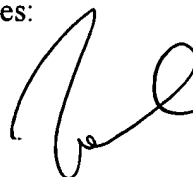
For the above reasons, it is believed that the rejections should be sustained.

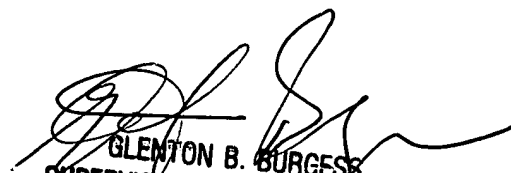
Respectfully submitted,

RR

September 12, 2005

Conferees:

 **JOHN FOLLANSBEE**
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

 **GLENTON B. BURGESS**
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100